

## UNITED STATES DISTRICT COURT

for the  
District of South Dakota

In the Matter of the Search of: )  
 The property located [REDACTED] )  
 [REDACTED] Box Elder, South Dakota, 57719, )  
 and to search any curtilage, storage units, )  
 persons and vehicles on the premises and )  
 associated with Apartment C, as well as the )  
 content of any computer and electronic storage )  
 devices )

Case No. 5:20-mj-68

REDACTED

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE "ATTACHMENTS A, C, and D", which is attached to and incorporated in this Application and Affidavit, located in the District of South Dakota, there is now concealed (*identify the person or describe the property to be seized*):

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2251, 2252, and 2252A& 18 U.S.C. § 2422(b)	Possession, Receipt, Distribution, and Production of Child Pornography & Enticement of a Minor Using the Internet

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.  
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.  
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.


Sworn to before me and: ☒ signed in my presence.

☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 3-23-2020

City and state: Rapid City, SD

  
 SSA Brent Gromer, SD DCI & FBI TFO

  
 Judge's signature

Daneta Wollmann, U.S. Magistrate  
 Printed name and title

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:

The property located at [REDACTED]  
[REDACTED] Box Elder, South  
Dakota, 57719, and to search any  
curtilage, storage units, persons and  
vehicles on the premises and associated  
with Apartment C, as well as the content  
of any computer and electronic storage  
devices

CASE NUMBER: 5:20-mj-68

**AFFIDAVIT IN SUPPORT OF  
SEARCH WARRANT  
APPLICATION**

**REDACTED**

[illegible]

I, Brent Gromer, being duly sworn, state as follows:

1. I am a Supervisory Special Agent with the South Dakota Division of Criminal Investigation. I have been employed as a Law Enforcement Officer in the State of South Dakota for over 23 years. In 2018, I became a Task Force Officer (TFO) for the Federal Bureau of Investigation. I have been involved in numerous investigations into all manner of crime. I have received training in Search and Seizure from the South Dakota Attorney General's Office, United States Attorney's Office, the United States Drug Enforcement Administration, Federal Bureau of Investigation and other private training organizations. I have personally prepared numerous affidavits in support of request for search

warrant. State and Federal courts have granted search warrants based on those affidavits that have withstood suppression efforts.

2. Since June of 2010, I have been assigned to the Internet Crimes Against Children (ICAC) Task Force in South Dakota. During that time, I have received additional training in collecting, preserving and analyzing evidence stored in different digital formats. The following is a list of specialized training I have received in conducting digital investigations and digital forensic examinations:

- Peer-to-Peer Computer Investigations
- Access Data BootCamp
- ICAC Unit Supervisor
- Internet Forensics
- Windows 7 Forensics
- Internet Relay Chat
- MAC Forensics
- Basic Data Recovery and Acquisition
- Intermediate Data Recovery and Acquisition
- Secure Techniques for On-Scene Preview
- Identification and Seizure of Electronic Evidence
- ICAC Ares
- Child Exploitation
- ICAC eMule Investigations
- Child Pornography the Ultimate Tool to Rescue Children
- ICAC BitTorrent Investigations
- Identification of Child Sex Trafficking
- NUIX Basic
- Cybertip Management
- 2014 Techno Security Conference
- 2015 National ICAC Conference
- 2015 Crimes Against Children Conference
- Android Open Source Forensics – Epyx Forensics
- Online Ads Investigations
- Undercover Chat Investigations
- Forensics Investigations with NetClean/Griffeye Analyze
- 2016 National ICAC Conference
- 2016 State of the States Cyber Crime Conference
- 2016 Florida ICAC Symposium

- 2017 Association of State Criminal Investigative Agencies
- 2017 Sex Offender Registry Conference
- 2017 South Dakota Technology Teachers Conference
- 2017 US Attorney's Office Law Enforcement Coordinating Committee Training Seminar
- 2017 South Dakota Society for Technology in Education Conference
- Cellebrite Training
- 2018 Appointed as a Special Deputy US Marshall under the Federal Bureau of Investigation
- Co-Chair National Internet Crimes Against Child Emerging Technology Committee
- South Dakota Center for the Prevention of Child Maltreatment Advisory Board Member.
- Griffeye Analyze DI Training.

3. In addition to the training I have received, I have presented to numerous professional groups and organizations and have testified as an expert on numerous occasions in US District Court, US Magistrate Court, and South Dakota Circuit Court.

4. During my law enforcement career, I have been involved in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A and enticement of a minor using the internet in violation of 18 U.S.C. § 2422(b). I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and enticement of a minor using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

5. I am aware that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of visual depictions of a minor engaging in sexually explicit conduct, using any means or facility of

interstate or foreign commerce, including by computer or utilizing the internet. I am also aware that 18 U.S.C. § 2422(b) criminalizes enticement of a person under 18 to engage in unlawful sex acts utilizing the internet.

6. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no information known to me that would tend to negate probable cause has been withheld from this affidavit.

**ITEMS TO BE SEARCHED FOR AND SEIZED:**

7. This affidavit is submitted in support of an application for a search warrant for the property located at [REDACTED], Box Elder, South Dakota, 57719, further described as a multiple occupant apartment building located on the intersection of W Gate Rd and Cardinal Drive, with two entrances to the building; the main entrance faces South and back entrance faces North. [REDACTED] is located on the first floor. It is the last apartment on the West side (left) if entering from the main entrance. The letter "[REDACTED]" is clearly visible on the brown wooden door of [REDACTED]. As of March



19th, there is a green clover hanging on the door beneath the letter "■" (hereinafter also referred to as SUBJECT PREMISES and photographically depicted in Attachments C-E). Additionally, your affiant seeks the warrant authorize the search of any vehicles, storage units and curtilage of the ■■■■■; any persons on the property; and the content of any computer and electronic storage devices, cellular phones, tablets, and any other electronic storage devices, including but not limited to external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities. I respectfully request the Court permit law enforcement to seize all such electronic devices located on the premises and further, to access and search the contents of said electronic devices without seeking an additional or separate warrant.

8. The warrant is being obtained in order to search for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A, which criminalize the production, distribution, receipt and possession of child pornography and 18 U.S.C. § 2422(b), which criminalizes enticement of a minor using the internet.

#### **DEFINITIONS**

9. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text

communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography

in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and



related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when

touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. “Electronic Storage Device” includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

l. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

m. “Hash value,” as used herein, refers to a unique alphanumeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file’s content. A hash value is a

file's "digital fingerprint." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

n. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address is one of two versions. Internet Protocol Version 4 (IPV4) or Internet Protocol Version 6 (IPV6). IPV4 looks like a series of four numbers, each in the range 1-255, separated by periods. IPV6 looks like a series of 8 numbers or letters separated by a colon. Each series of numbers will be 0-9 and/or a-f. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be properly directed from its source to its destination. Most Internet Service Providers (ISPs – defined below) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs

o. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

p. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

**BACKGROUND ON CHILD PORNOGRAPHY,  
COMPUTERS, THE INTERNET, AND EMAIL**

10. I have training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format

directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices



include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

11. Based upon my training and experience, as well as information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during a search of physical premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it

is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image

files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

12. Based on my training and experience, as well as my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require

particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

13. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable

evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

#### **PROBABLE CAUSE AND BACKGROUND OF THE INVESTIGATION**

14. On February 24, 2020, Special Agent Kristopher Serra, Federal Bureau of Investigation (FBI) assigned in New York state, was working in an undercover capacity on Kik Messaging Service, a social networking, internet application. SA Serra was in a Kik Group titled "Family fun room (No limits)." SA Serra received a private message from Kik user "Ranger\_danger89," later identified as Adam Ryan Swift, Box Elder, South Dakota. The name associated with Ranger\_danger89 was listed as "Adam Ryan." During the



conversation via Kik Messenger, "Adam Ryan" and SA Serra's undercover persona (hereinafter "UC") discussed being "active." I know that "Active" is a chat term used to describe people who are sexually active, usually meaning with children. During the conversation, "Adam Ryan" stated that he was "active" with his 4-year-old son and 7-year-old stepson. The UC advised "Adam Ryan" they were "active" with their 9-year-old stepchild. As the conversation continued, they wrote about where each of them lived. The UC Persona advised "Adam Ryan" that he lived in New York. "Adam Ryan" stated he lived in the United States but did not immediately identify where. "Adam Ryan" asked the UC for photographs of the alleged UC persona's 9-year-old stepchild. The UC stated he had only clothed images, as he did not keep "nudes" on his phone. The UC asked "Ryan" if he had photos. "Adam Ryan" replied "Same. Clothed except one of my stepson." "Adam Ryan" then sent a photograph of himself that appeared to have been taken in a vehicle. There is a young boy visible in the back seat of the vehicle in a child restraint seat. "Adam Ryan" sent a second photograph of a young boy taken in what appears to be a grocery store and the child is sitting in a shopping cart.

15. The conversation continued and the UC asked "Adam Ryan" if he preferred "boys or girls." "Adam Ryan" replied "Both." "Adam Ryan" asked the UC what he preferred. The UC informed him that he had a little girl, but had never been with a boy. "Adam Ryan" asked the UC to send photographs of the girl. The UC then sent the UC photograph of a female child. The UC had previously identified that age of the "girl" as 9 years old. After the UC

complied with “Adam Ryan’s” request for photos of his 9-year-old step-daughter, “Adam Ryan” replied “Yummy, I love them younger than that!” “Adam Ryan” asked the UC what he had done with the girl. The UC responded, in a manner implying the UC had engaged in sexual penetration with the child. The UC asked “Adam Ryan”, “You got any vids?” “Adam Ryan” initially responded that he did not have any of him. The UC then asked for “anything young?” Ryan then sent a video titled:

**Bdd7beac-af8a-4cef-82a3-67e1052ad1f4.mp4** – This is a 1:49 video of an adult male and a female child who appears to be approximately 10-12 years of age. When the video begins the child is lying on her left side and the male is positioned near her buttocks on his knees. The male is masturbating. 6 seconds into the video the video scene changes and the child is seen on her back with her legs spread and the adult male is vaginally raping her with his penis. The rape continues through 1:15 in the video when the scene again changes to the male masturbating and ejaculating on the child’s face.

16. Thereafter, the UC commented about the high-heeled shoes the girl wore in the video. The UC then asked “Adam Ryan” where in the United States he was located. “Adam Ryan” sent a second video titled:

**933552a1-21f8-4b0b-b502-f13b3390aada.mp4** – This is a 36 second video of a female child who appears to be approximately 5-7 years of age. The video shows the female child being orally raped by an adult

penis. This continues to 32 seconds into the video when the camera pans to the child's buttocks.

17. After sending the two videos, "Adam Ryan" responded to the UC's question asking where he lived in the United States. "Adam Ryan" replied "South Dakota." The conversation continued and the UC asked "Adam Ryan" "Whats (sic) your youngest." "Adam Ryan" replied, "My son was 2 when I sucked him. I ate out a newborn girl fairly often. I babysat her for about a year. Licked her pussy all the time." The conversation continued and "Adam Ryan" and the UC discussed whether their wives knew of what they were doing and both stated the wives did not know. The conversation concluded on February 24, 2020.

18. SA Serra prepared a report and sent that to SA Erik Doell, FBI Rapid City. SA Doell contacted me and asked if the SD ICAC Task Force would conduct the follow up investigation. SA Doell provided me the report prepared by SA Serra and the results of SA Serra's investigation. SA Serra had prepared a subpoena for the IP addresses used to access Kik Messaging Service from February 11, 2020, through February 24, 2020. Kik Messaging service provided a list of IP Addresses. The user accessing the Ranger\_danger89 account was accessing Kik Messenger through IP Address 24.111.189.122, which Midcontinent Communication owns. SA Serra had sent a subpoena to Midcontinent for the subscriber information for the lessee of this IP Address on February 24, 2020. Midcontinent responded that the

lessee of the IP Address was Fox Den Store-It, located at 12192 Siouxland Rd., Summerset, SD.

19. In addition to the IP information, Kik Messenger identified [aswift889@gmail.com](mailto:aswift889@gmail.com) as the email address associated with the Ranger\_danger89 account.

20. I conducted a search of local records for Adam Swift based on the information received from Kik Messenger and Midcontinent Communication. I located local resident:

Adam Ryan Swift  
[REDACTED]  
Box Elder, SD 57719  
DOB: [REDACTED]/89

21. I conducted a search of Facebook.com and located a publicly accessible page belonging to Adam Swift. In review of the information listed on Adam Swift's Facebook page, I learned that Adam Swift listed he was a sales manager for Fox Den Store-it in Summerset, SD, the same location where "Adam Ryan" accessed the Ranger\_Danger89 Kik Messenger account. Through further examination of the information provided by SA Serra and the information on Swift's Facebook page, I located the same photograph in Facebook as was used for the profile photograph for Ranger\_danger89.

22. I then contacted United States Homeland Security Investigations Special Agent Scott Beagle. SA Beagle commonly works on line in an undercover capacity. I asked SA Beagle to offer Swift the opportunity to communicate with him via Kik Messaging Service. SA Beagle introduced

himself to Swift, via the Ranger\_danger89 Kik user account on March 10, 2020, writing, "24f.26m.5yo.active fam here", meaning, the "family" was made up of a 24-year-old female, a 26-year-old male and a 5-year-old child who were "active" as described above. Swift thereafter responded. During the conversation, SA Beagle portrayed himself as a 24-year-old female with a 5-year-old daughter. Swift informed SA Beagle's UC Persona that he was engaged to be married and had two children, ages 4 and 6. During the conversation SA Beagle and Swift exchanged photographs. The photograph provided by Swift again matched the previously described photographic identification. SA Beagle asked Swift, "So what r u into? Looking for?" Swift replied "Into anything no limits. Looking for other taboo families and ideally one that would let me use their daughter one day." SA Beagle's UC persona stated they have let "outsiders in for our daughter" and reminded him the "daughter" was 5 years old. Swift replied, "I love it" then added, "The youngest I've had was 3." SA Beagle's persona asked about Swift's experience. Swift wrote, "Friends (sic) kid and being raised that way." A couple of messages later SA Beagle's persona asked Swift if he was "active" and if he was serious about meeting with the UC persona's daughter. Swift replied, "Yes I'm serious and active". SA Beagle's persona asked Swift with whom he was "active". Swift wrote he was "active" with his son and later added, "I suck him". Swift and SA Beagle's persona wrote about how long each of them had been "active" and how they had begun in the "lifestyle". As the conversation continued, SA Beagle's persona asked Swift what Swift

wanted to do with the UC's "daughter". Swift replied, "I'd love to eat her out and fuck her pussy". SA Beagle's persona again reminded Swift the child was only 5 years old and not allowed to engage in penetration. Swift then wrote, "I'll eat her out as much as I can". Swift asked SA Beagle's persona, "So you don't want to do anything with my son?" Swift told SA Beagle's persona that she could do "anything you want", and added "I want to watch you suck him". Swift and the UC wrote about whether their significant others knew about the abuse with the children. Swift advised his fiancé did not know he was abusing his son. As the conversation continued, Swift asked the UC for photographs of the child. At Swift's prompting, they also discussed arranging a time to meet and "swap" the children. They talked about a workable schedule for the meeting. They set Friday, March 20, 2020, as the potential for an initial meeting date.

23. Swift continued to write about what the child would like. He asked the UC, "She enjoy being ate out?" When the UC replied, "Yes". Swift wrote, "Good! I want her sitting on my face". Swift asked the UC if he would allow "gentle fingering" of the girl. Swift went on and asked the UC "She suck (sic) cock yet?"

24. The conversation continued and the UC and Swift further discussed being in the "lifestyle". Swift informed the UC, "I was used by my dad and brother and was allowed to eat my sister out but never allowed to fuck her." The conversation continued and the UC mentioned a Kik group to which he belonged and Swift asked if he wanted to join. When Swift answered



affirmatively, the UC stated Swift could, but that Swift would have to “verify.” I know that “verify” means to send a proof-of-life-type video to show the person is not law enforcement. Swift agreed and sent a video of himself to the UC. In the video, Swift was in a car talking to the camera and stated, among other things that, “Today is March 10<sup>th</sup>”.

25. During the conversation, Swift and the UC also wrote about what each other did for jobs. Swift informed the UC that he was a Manager at Fox Den Store-it. Swift asked the UC several questions about “her and her husband” and “the lifestyle”. Swift told the UC, “I think you’ll love sucking on my son. He loves having it done!” He told the UC, “He likes to moan and place his hand on my head while I do it”. When the UC questioned him about the veracity of this statement, Swift explained, “It’s just an orgasmic moan. It’s just a simple moan”. Swift asked the UC if “she” wanted him to “prove it”. The UC discouraged Swift from proving he was sexually abusing his son. The conversation on March 10, 2020, concluded shortly after.

26. The UC Persona talked about possible meeting dates with Swift, however Swift wrote that he was going to be out of state in Wisconsin until Saturday, 3/14/20. SA Beagle monitored the Ranger\_Danger89 account, but found that Swift had not accessed the account until 3/19/20 when the conversation continued.

27. On March 19, 2020, SA Beagle received additional messages from Swift via Kik Messenger. Swift told the UC that he had just gotten back and asked the UC “how’s your princess”. The UC asked Swift if it still worked to

meet on March 20, 2020. Swift replied, "To show you video and pics?" The UC then wrote that he meant for the previously discussed meeting on March 20, 2020. Swift then said he could not meet on March 20, 2020 because he had to work until 8 pm. He said he would be available to meet over the weekend of March 21, 2020 and March 22, 2020. The UC asked Swift what he meant by sending pics and vids". Swift explained, "I can send you pictures and videos of my son while I play with him". Again, the UC discouraged Swift from doing that. Swift added that he would be off on Wednesday, March 25, 2020, and would be available to meet then. Swift informed the UC that he would create live videos while he abused his son or would do a live chat while he abused his son. The UC corrected him about dates available for meeting and Swift wrote that he liked a woman who "took charge". The UC informed him that she was not into him. Swift replied, "I know that", "And you aren't really my type, I just like when women take charge". Swift then told the UC, "I can't wait to taste your princess's pussy". The UC suggested when they met for the first time, that Swift leave his son at home and Swift could just meet with the UC's daughter. Swift wrote "Yeah? I'd love that!", and added "Have you watch me use her as my own little fuck toy", "Think she would enjoy my tongue?". The UC Persona asked Swift if he would be able to meet right away. Swift said he wished that he could, but indicated he was currently working. They then agreed that Swift would contact the UC at approximately 5:00 pm Mountain time on March 19, 2020.

28. On March 19, 2020, Homeland Security Resident Agent in Charge (RAC) Nick Saroff, conducted surveillance in the area of Fox Den Store-It in Summerset, SD, the location of which the IP address to the Ranger\_danger89 Kik account returned. He was not able to confirm that Swift was at the business as he said that he would. SA Michelle Pohlen, HSI, conducted surveillance in the area of Swift's residence. She was not able to locate Swift's vehicle at that time. She did verify the property information set forth above and obtained the photographic warrant attachments. On March 12, 2020, SA Pohlen also surveilled Swift's apartment complex and located his vehicle, a gray Ford Fusion bearing SD Veteran's Lic.: 0973G. On March 19, 2020, SA Pohlen checked the area of Fox Den Store-It at 2810 Eglin St., Rapid City. She located Swift's gray Ford Fusion and she was able to see Swift inside of the business as she conducted surveillance.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE  
A SEXUAL INTEREST IN CHILDREN AND/OR WHO  
PRODUCE, RECEIVE AND/OR POSSESS CHILD  
PORNOGRAPHY**

29. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

- a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children,

or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines,

correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the

investigation of child pornography throughout the world. Thus, even if Adam Swift uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as well as on electronic devices found in the home, as previously detailed and as set forth in Attachment A.

**REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT**

30. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the target an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

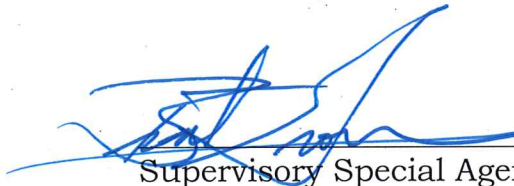
**CONCLUSION**

31. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, are located at the SUBJECT PREMISES, described further in Attachment A. I respectfully request that this Court issue



a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

32. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



Supervisory Special Agent Brent Gromer  
SD DCI and SD ICAC Commander  
FBI TFO

SUBSCRIBED and SWORN to



\_\_\_\_\_ in my presence  
\_\_\_\_\_ by reliable electronic means

this 23<sup>rd</sup> day of March, 2020.



DANETA WOLLMANN  
U.S. MAGISTRATE JUDGE

**ATTACHMENT A**  
**Property to Be Searched**

- The property located at [REDACTED], Box Elder, South Dakota, 57719, further described as a multiple occupant apartment building located on the intersection of W Gate Rd and Cardinal Drive, with two entrances to the building; the main entrance faces South and back entrance faces North. [REDACTED] is located on the first floor. It is the last apartment on the West side (left) if entering from the main entrance. The letter "■" is clearly visible on the brown wooden door of [REDACTED]. As of March 19th, there is a green clover hanging on the door beneath the letter "■" (photographically depicted in Attachments C-E);
- any vehicles associated with the occupants of apartment ■;
- storage units associated with apartment ■;
- the curtilage of the property associated with apartment ■;
- and any persons on the premises associated with apartment ■;
- the content of any seized computer and electronic storage devices, cellular phones, tablets, and any other electronic storage devices, including but not limited to external and internal and external hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities.

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A and 2422(b):

1. Computers, cell phones or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that

the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of 616 Cardinal Drive, Apartment C, Box Elder, South Dakota, 57719, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

c. Records and information relating to sexual exploitation of children, including correspondence and communications between various Seller and Buyer Accounts.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage

(such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies, CDs, DVDs).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which records computer data. Examples include external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, hard disks, RAM, flash memory, CDs, DVDs, and other magnetic or optical media.



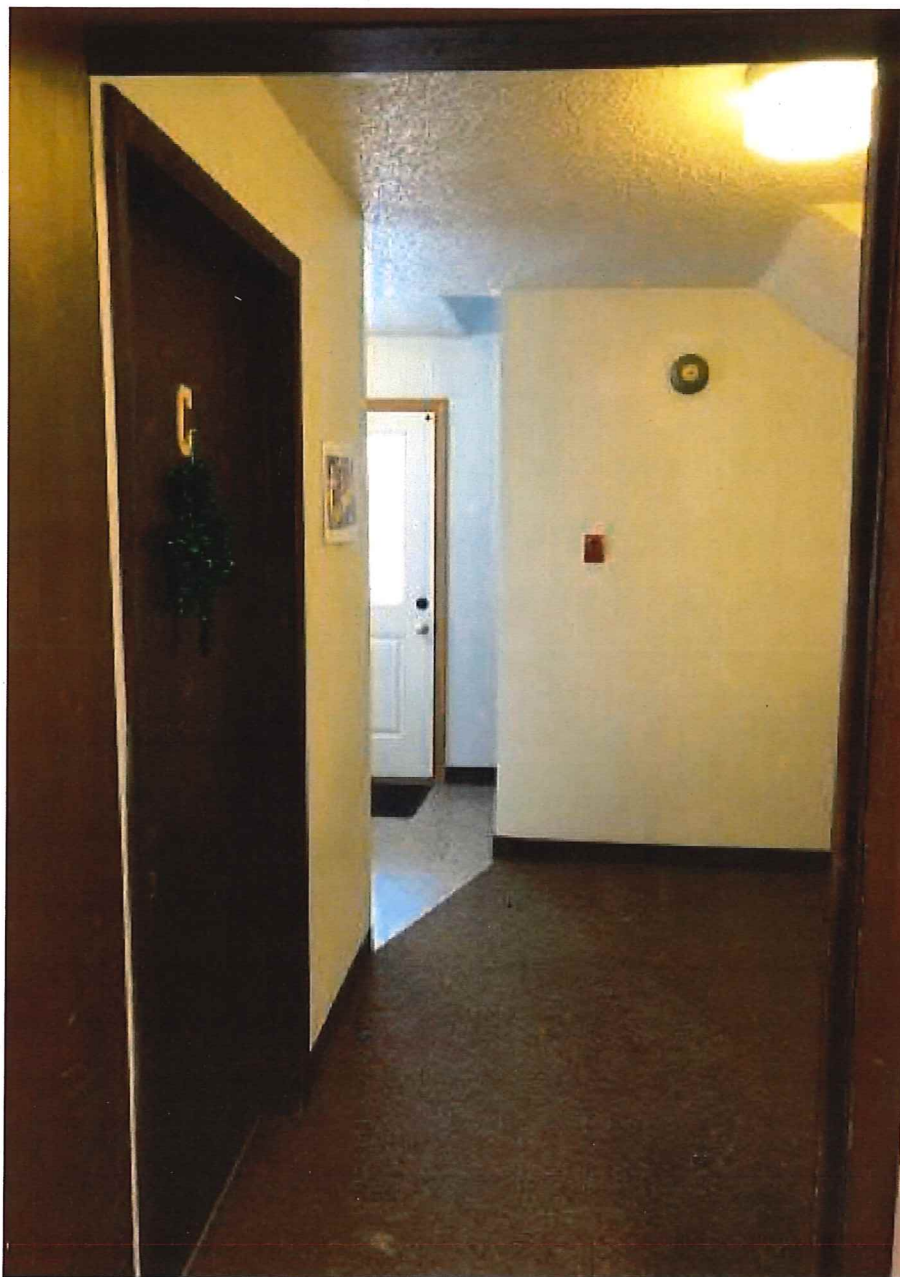
**ATTACHMENT C**





**ATTACHMENT D**





**ATTACHMENT E**

## UNITED STATES DISTRICT COURT

for the  
District of South Dakota

In the Matter of the Search of:

The property located [REDACTED]  
 [REDACTED] Box Elder, South Dakota, 57719,  
 and to search any curtilage, storage units,  
 persons and vehicles on the premises and  
 associated with Apartment C, as well as the  
 content of any computer and electronic storage  
 devices

Case No. 5:20-mj-68

REDACTED

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See ATTACHMENT A, C, and D, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, and 2252A, as described in ATTACHMENT B, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before April 6, 2020 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.  
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 3-23-2020 10:05pm


Judge's signature

City and state: Rapid City, SDDaneta Wollmann, U.S. Magistrate

Printed name and title



**Return**

Case No.:

5:20-mj-68

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*